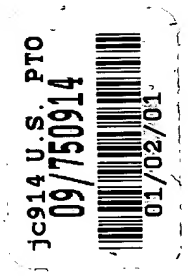
PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



In re application of

Makiba SHIGEZUMI

Serial No. (unknown)

Filed herewith

DNS SERVER FILTER

CLAIM FOR FOREIGN PRIORITY UNDER 35 U.S.C. 119 AND SUBMISSION OF PRIORITY DOCUMENT

Assistant Commissioner for Patents

Washington, D.C. 20231

Sir:

Attached hereto is a certified copy of applicant's corresponding patent application filed in Japan on January 21, 2000, under No. 12757/2000.

Applicant herewith claims the benefit of the priority filing date of the above-identified application for the above-entitled U.S. application under the provisions of 35 U.S.C. 119.

Respectfully submitted,

YOUNG & THOMPSON

By Benoît Castel

Benoît Castel
Attorney for Applicant
Customer No. 000466
Registration No. 35,041
745 South 23rd Street
Arlington, VA 22202
Telephone: 703/521-2297

January 2, 2001

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　１月２１日

出願番号
Application Number: 特願２０００－０１２７５７

出願人
Applicant (s): 日本電気株式会社

２０００年　９月２２日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願
【整理番号】　65000524
【提出日】　平成12年 1月21日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L 12/66
G06F 13/00
H04L 12/46
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　重住　牧
【特許出願人】
【識別番号】　000004237
【氏名又は名称】　日本電気株式会社
【代理人】
【識別番号】　100080816
【弁理士】
【氏名又は名称】　加藤　朝道
【電話番号】　045-476-1131
【手数料の表示】
【予納台帳番号】　030362
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9304371
【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　ＤＮＳサーバフィルタ

【特許請求の範囲】

【請求項１】

受信したＤＮＳ（Domain Name System）パケットについて、該パケットをＤＮＳサーバに渡すまえに、該パケットの内容に異常があるか否か検査するパケット検証手段を備え、異常を検出した際にエラー応答パケットを生成して要求元に返す、ことを特徴とするＤＮＳサーバフィルタ装置。

【請求項２】

組織外の者が組織外のネットワークから送信するホスト名、ドメイン名、ＩＰ（Internet Protocol）アドレスに関する情報をＤＮＳプロトコルを通じて取得するためのＤＮＳパケットを前記パケット検証手段で検査し、異常があればエラー応答を返し、組織外の者が組織のネットワーク構成情報を利用して組織のネットワークに侵入を行うこと、及び、異常な形式のパケットを受信することでＤＮＳサーバが動作異常になること、を未然に防ぐようした、ことを特徴とする請求項１記載のＤＮＳサーバフィルタ装置。

【請求項３】

組織内の端末から組織外のネットワークに属するＤＮＳサーバに送信するホスト名、ドメイン名、ＩＰアドレスに関する情報をＤＮＳプロトコルを通じて取得するためのＤＮＳパケットを、前記パケット検証手段で検査し、異常があればエラー応答を返し、組織外のネットワークに属するＤＮＳサーバを動作異常とさせることを未然に防ぐようにした、ことを特徴とする請求項１記載のＤＮＳサーバフィルタ装置。

【請求項４】

前記パケット検証手段によるパケットの異常検出の条件について、追加、及び削除自在とされている、ことを特徴とする請求項１乃至３のいずれか一に記載のＤＮＳサーバフィルタ装置。

【請求項５】

請求項１乃至４のいずれか一に記載の前記ＤＮＳサーバフィルタ装置を、ファ

イアウォール装置内に実装し、

前記ファイアウォール装置の前記ＤＮＳサーバフィルタ装置は、前記ファイアウォール装置が設置される組織の管理外の第１のネットワークと、組織内の第２のネットワークとをセキュリティを保ちながら相互接続し、ＤＮＳについて、前記第１のネットワークに属する端末が前記第２のネットワークに属する端末のホスト名とＩＰアドレスの情報やネットワークの名前空間に関する情報を取得すること、

前記第１のネットワークに属する端末から前記第１のネットワークを通じてＤＮＳサーバに対してＤＮＳプロトコル上不正なパケットを送付してＤＮＳサーバに動作異常を引き起こすこと、

前記第２のネットワークに属する端末やＤＮＳサーバが前記第１のネットワークに属する端末や前記第１のネットワークに属するホストに対してＤＮＳプロトコル上異常なパケットを送付すること、

を防ぐようにした、ことを特徴とするファイアウォール装置。

【請求項６】

パケットフィルタリング型のファイアウォール装置と、

ファイアウォール装置と通信接続する請求項１乃至４のいずれか一に記載の前記ＤＮＳパケットフィルタ装置と、

前記ＤＮＳパケットフィルタ装置と通信接続するＤＮＳサーバと、を備えたことを特徴とするネットワークシステム。

【請求項７】

ＤＮＳプロトコルにおける端末及びＤＮＳサーバからの問い合わせ、及び、ＤＮＳサーバからの応答パケットを受信するパケット受信部と、

問い合わせ要求を管理するためのセション管理テーブルを備え、問い合わせ及び応答パケットを管理し全体の制御を行うセション管理部と、

問い合わせ及び応答パケットが異常であるか否かを検査するパケット検証部と、

ＤＮＳサーバへの問い合わせパケットを生成する要求生成部と、

問い合わせパケットの送信元に返す応答パケットを生成する応答生成部と、

問い合わせ及び応答パケットを送信するパケット送信部と、

を備え、受信したＤＮＳプロトコルのパケットについて該パケットをＤＮＳサーバに渡すまえに、内容に異常があるか否か検査し、異常を検出した際に、エラー応答パケット生成して要求元に返す、ことを特徴とするＤＮＳサーバフィルタ装置。

【請求項８】

前記パケット検証部が、

検証プログラムのエントリポイントアドレス情報と、検証プログラムの実行の優先順位情報と、検証プログラムの属性情報とを備えたプログラム管理テーブルを備え、前記検証プログラムの属性を参照し、実行すべき検証プログラムを選択して実行に移す制御を行う呼出管理部と、

検証プログラムを格納した記憶装置と、

管理ツールもしくは設定ファイルで指示された検証プログラムの実行ファイルをメモリ上にロードし、ロードされた検証プログラムを初期化し、検証プログラムのエントリポイントを、入手した属性と共に、前記呼出管理部のプログラム管理テーブルに登録し、前記管理ツールで削除が指示された検証プログラムをメモリ上から解放処理を行うように制御するロード管理部と、

実行される検証プログラムから呼び出されるＤＮＳサーバフィルタ本体の機能を利用するためのサブルーチン群よりなるサービスルーチンと、

を備えている、ことを特徴とする請求項７記載のＤＮＳサーバフィルタ装置。

【請求項９】

前記セション管理テーブルが、要求パケットへのポインタと、問い合わせ要求を行った要求元のＩＰアドレスと、問い合わせ要求を行った要求元ポート番号と、問い合わせ要求のパケット形式が正常であった場合に問い合わせ要求を別のＤＮＳサーバに転送しているかどうかを示すフラグと、を備え、

前記パケット受信部が、ＤＮＳパケットを受信すると、該パケットを前記セション管理部に渡し、

前記セション管理部は、前記セション管理テーブルに、受信したパケットの送信元のＩＰアドレス、受信したパケットのポート番号を設定し、テスト中を意味

する値をフラグを設定したのち、受信パケットを、前記パケット検証部に渡してパケットの検査を依頼し、

前記パケット検証部で前記受信パケットの検査を行った結果、検査結果に問題がある場合、前記セション管理部が、前記受信パケットの種別を調べて、問い合わせ要求であるか否か判定し、問い合わせ要求であれば、前記セション管理部は、前記応答生成部に対して、エラー応答パケットの生成を依頼し、

生成されたパケットを、前記セション管理テーブルの要求元ＩＰアドレス、ポート番号で指定される相手に対して、前記パケット送信部に送信を依頼し、受信したパケットについて、前記セション管理テーブルに登録されている情報を削除して、受信した問い合わせ要求パケットを解放し、

受信パケットが問い合わせ要求でない場合には、前記セション管理部は、前記セション管理テーブルを検索して、元の問い合わせ要求に関する部分を取り出し、検索された前記セション管理テーブルのエントリの要求パケットへのポインタから、問い合わせ要求パケットを参照して、これを基に、前記応答生成部に対して、エラー応答パケットの生成を依頼し、前記セション管理テーブルの要求元ＩＰアドレス、及びポート番号で指定される相手に対して、生成した応答パケットを送信するように、前記パケット送信部に対して依頼し、受信した応答パケットについて、前記セション管理テーブルに登録されている情報を削除して応答パケットを解放するとともに、該応答パケットに対応する問い合わせ要求について、前記セション管理テーブルに登録されているエントリも削除する、ことを特徴とする請求項８記載のＤＮＳサーバフィルタ装置。

【請求項１０】

前記パケット検証部でパケットの検査を行い、検査結果に問題がない場合、前記セション管理部が受信パケットの種別を調べ、応答パケットの場合、前記セション管理部は、該応答パケットに対応する問い合わせ要求の情報を、前記セション管理テーブルから検索し、前記セション管理部が受信した応答パケットが元の問い合わせ要求に対する回答となっているかどうかを調べ、

前記調査の結果、さらに問い合わせを行う必要があれば、前記セション管理部は、受信した応答パケットの情報から次の問い合わせ先を決定して、前記要求生

成部に問い合わせ要求パケットの生成を依頼し、前記パケット送信部に対して次の問い合わせ先への送信を依頼し、

前記セション管理部は、受信した問い合わせの途中経過である応答パケットに関する情報を、前記セション管理テーブルから削除して応答パケットを解放し、

前記調査の結果、元々の問い合わせパケットに対する回答となる応答パケットを受信した場合には、前記セション管理部は、応答パケットを受信した応答パケットの結果を反映させた元の問い合わせ要求に対する応答パケットの生成を前記応答生成部に依頼し、前記パケット送信部に元の問い合わせ要求の送信元に対して送信を依頼し、受信した応答パケットに関連する情報を前記セション管理テーブルから削除し、元の問い合わせ要求に関する情報を前記セション管理テーブルから削除し応答パケットを解放する、ことを特徴とする請求項９記載のＤＮＳサーバフィルタ装置。

【請求項１１】

前記パケット検証部でパケットの検査を行い、検査結果に問題がない場合、前記セション管理部が受信パケットの種別を調べ、受信したパケットが問い合わせ要求である場合、前記セション管理部が受信パケットの送信元を調べ、前記送信元が組織内部のネットワークからの問い合わせでない場合、組織外のネットワークの問い合わせ要求を解決するために前記セション管理部は、まず最初に問い合わせる組織外のＤＮＳサーバを決定し、元の問い合わせ要求を元にした問い合わせ要求の生成を前記要求生成部に依頼し、その問い合わせ要求パケットを、前記決定されたＤＮＳサーバに対して送信するようにパケット送信部に依頼し、

前記送信元が組織内部のネットワークからの問い合わせである場合、前記セション管理部は受信した問い合わせ要求パケットを元に要求生成部に問い合わせ要求パケットの生成を依頼し、ＤＮＳサーバに対する問い合わせパケットの送信を前記パケット送信部に依頼し、

前記セション管理部は、受信したパケットに対応する前記セション管理テーブルのエントリ中のフラグに、「問い合わせ中」の値を設定し、受信パケットへのポインタを前記セション管理テーブルのエントリのポインタに設定する、ことを特徴とする請求項９又は１０記載のＤＮＳサーバフィルタ装置。

【請求項１２】

ＤＮＳサーバ情報をあらかじめ蓄えておくキャッシュメモリを備えたことを特徴とする請求項７記載のＤＮＳサーバフィルタ装置。

【請求項１３】

（ａ）ＤＮＳプロトコルにおける端末及びＤＮＳサーバからの問い合わせ、及びＤＮＳサーバからの応答パケットを通信装置を介して受信するパケット受信処理と、

（ｂ）問い合わせ要求を管理するためのセション管理テーブルを備え、問い合わせ及び応答パケットを管理し全体の制御を行うセション管理処理と、

（ｃ）問い合わせ及び応答パケットが異常であるか否かを検査するパケット検証処理と、

（ｄ）ＤＮＳサーバへの問い合わせパケットを生成する要求生成処理と、

問い合わせパケットの送信元に返す応答パケットを生成する応答生成処理と、

（ｅ）問い合わせ及び応答パケットを通信装置を介して送信するように制御するパケット送信処理と、

を備え、受信したＤＮＳパケットについて該パケットをＤＮＳサーバに渡すまえに、内容に異常があるか否か検査し、異常を検出した際に、エラー応答パケット生成して返すという、ＤＮＳサーバフィルタの処理を、コンピュータ上で実行させるためのプログラムを記録した記録媒体。

【請求項１４】

請求項１３記載の記録媒体において、検証プログラムのエントリポイントアドレス情報と、検証プログラムの実行の優先順位情報と、検証プログラムの属性情報とを備えたプログラム管理テーブルを備え、

前記パケット検証処理が、前記検証ソフトウェアの属性を参照し、実行すべき検証プログラムを選択して実行に移す制御を行う呼出管理処理と、

管理ツールもしくは設定ファイルで指示された検証プログラムの実行ファイルをメモリ上にロードし、ロードされた検証プログラムを初期化し、検証プログラムのエントリポイントを入手した属性と共に前記プログラム管理テーブルに登録し、及び前記管理ツールで削除を指示された検証プログラムのメモリ上からの解

放処理を行うロード管理処理と、

検証プログラムから呼び出されるＤＮＳサーバフィルタ本体の機能を利用するためのサブルーチン群よりなるサービスルーチン処理と、

の各処理を、前記コンピュータ上で実行させるためのプログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークシステムに関し、特に、ＩＰアドレスとドメイン名との対応の管理を行うドメインネームシステム（ＤＮＳ）のフィルタ装置に関する。

【０００２】

【従来の技術】

ＤＮＳ（Domain Name System）は、インターネット等のＴＣＰ／ＩＰ（Transport Control Protocol/Internet Protocol）を用いたプロトコル（トランスポート層としてＵＤＰ（User Datagram Protocol）も含む）によるネットワークにおいて接続されたホストの名前とＩＰアドレスとを関連付けた情報等をＴＣＰ／ＩＰネットワークに接続されたホストに提供する、ＴＣＰ／ＩＰプロトコル上のサービスである。ＤＮＳでは、ホストが属している組織に対してドメイン名と呼ばれる名前でまとめられており、ドメイン名は、国家レベル、企業、学術組織等の組織の種別毎、組織名毎、組織内の部署毎に階層的に名付けられ、ホスト名はドメイン名と組み合わせることで、ＴＣＰ／ＩＰネットワークにおける唯一性が保証される。例えば、インターネットに接続された日本の企業の日本電気株式会社のＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）サーバは、日本を示す“ｊｐ”、企業を示す“ｃｏ”、日本電気株式会社を示す“ｎｅｃ”、同社において名付けられたＷＷＷサーバのホスト名を示す“ｗｗｗ”を、“ｗｗｗ．ｎｅｃ．ｃｏ．ｊｐ”という記述方法で表現される。

【０００３】

“ｗｗｗ．ｎｅｃ．ｃｏ．ｊｐ”の“ｎｅｃ．ｃｏ．ｊｐ”はインターネット

におけるドメイン名割り当て機関であるＮＩＣ（Ｎｅｔｗｏｒｋ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｃｅｎｔｅｒ）により割り当てられた日本電気株式会社を示すドメイン名であり、“ｗｗｗ”は日本電気株式会社内で割り当てられたホスト名である。ＴＣＰ／ＩＰプロトコルで通信しようとするホストは、接続先のホストのＩＰアドレスを知らなければならず、このWWWサーバにＴＣＰ／ＩＰで接続しようとするインターネットに接続されたホストは、“ｗｗｗ．ｎｅｃ．ｃｏ．ｊｐ”という名前に対応するＩＰアドレスをＤＮＳサーバに問い合わせる。“ｗｗｗ．ｎｅｃ．ｃｏ．ｊｐ”に接続しようとするホストは、まずルートサーバと呼ばれるＤＮＳにおけるドメイン階層構造の頂点の情報を管理するＤＮＳサーバに問い合わせ、“ｊｐ”ドメインを管理しているＤＮＳサーバを教えてもらい、次にその“ｊｐ”ドメインを管理しているＤＮＳサーバに問い合わせ、“ｃｏ．ｊｐ”ドメインを管理しているＤＮＳサーバを教えてもらい、次に“ｃｏ．ｊｐ”ドメインを管理しているＤＮＳサーバに問い合わせ、“ｎｅｃ．ｃｏ．ｊｐ”を管理しているＤＮＳサーバを教えてもらい、次に“ｎｅｃ．ｃｏ．ｊｐ”ドメインを管理しているＤＮＳサーバに“ｗｗｗ．ｎｅｃ．ｃｏ．ｊｐ”というホスト名に対するＩＰアドレスを問い合わせ、そのＤＮＳサーバにその名前があればこのホストのＩＰアドレスを返す。

【０００４】

インターネットに接続する組織において、セキュリティ上の理由により、インターネットに接続する部分にファイアウォールを設置して、直接、ＴＣＰ／ＩＰプロトコルによる組織外との通信を制限する場合がある。

【０００５】

組織のセキュリティ要件として、組織外秘の情報の保護の為に組織外からのＴＣＰ／ＩＰプロトコルを通じた組織内資源へのアクセスを制限することが挙げられる。

【０００６】

ＤＮＳにおいても、組織内のネットワークに接続されたホストの名前やＩＰアドレスについての情報やその組織の部署名やネットワーク構成が名付けられているドメイン名をできる限り隠すことによって、侵入者がこの情報を用いて、組織

内のネットワークに侵入することを防ぐことが要請されている。

【０００７】

【発明が解決しようとする課題】

上記要請に対して、従来のシステムでは、組織内のＤＮＳサーバとは別にファイアウォールの外に設置された組織外のホストからのアクセスを許可するホストに関する情報を提供するＤＮＳサーバを設置し、組織内のＤＮＳサーバは、組織内のホストが組織外のホストのＤＮＳ情報を取得するためにファイアウォールの外に設置されたＤＮＳサーバに対して、再帰的に問い合わせできるように設定し、ファイアウォールの外に設置されたＤＮＳサーバから、組織内のＤＮＳサーバに対しては、問い合わせができないように、ＤＮＳサーバ及びファイアウォールに設定することで対処している。

【０００８】

かかる構成の従来のシステムにおいては、ＤＮＳサーバを複数台設置することや、ＤＮＳサーバの管理が複雑化する、といった問題点が生じている。

【０００９】

また、セキュリティ上の問題としては、不正な形式のパケットを攻撃対象のサーバに送信する事で、バグ等のサーバプログラムの実装上の問題によりサービスが停止させる「ＤｏＳ（Ｄｅｎｉａｌ　ｏｆ　Ｓｅｒｖｉｃｅ）アタック」と呼ばれる攻撃に対しても防御が必要となり、ＤＮＳサービスについても指摘されている。

【００１０】

従来、このような問題が指摘されると、サービスプログラムの開発者が、サービスプログラムを修正する必要があった。

【００１１】

たしかに、一部のサービスプログラムは、そのプログラムのソースファイルが公開されているため（ＵＮＩＸ™用ｂｉｎｄ等）、サービスプログラムの利用者がソースに対する修正差分を入手するか、利用者が修正を行ってコンパイルすることで、サービスプログラムをＤｏＳアタックに対応するものに交換することが可能とされている。

【００１２】

しかしながら、ソースファイルが公開されていない場合（例えばＭｉｃｒｏｓｏｆｔ社製Ｗｉｎｄｏｗｓ　ＮＴ　Ｓｅｒｖｅｒ　４．０に含まれるＤＮＳサーバ等の場合）、サービスプログラム開発者が修正モジュールをサービスプログラム利用者に配布するまでに時間を要し、ＤｏＳアタック等の問題が指摘されてから長い間、この問題に対して、適切な対処を施すことができない状態にあった。

【００１３】

またソースファイルが公開されていても、利用者自身のプログラミングスキルの不足等の理由により、適切に対処できない場合もある。

【００１４】

以上、ＤｏＳアタックについて説明したが、サービスは停止しないにしても、サービスプログラムの実装上の問題により、本来得られるべき正常な応答が返らない場合も、同様の問題が発生する。

【００１５】

また、組織のネットワークセキュリティ管理上、組織内部から組織外のホストに対してセキュリティ上脅威となる攻撃を行うことが可能とならないように、対策を施さなければならないといったセキュリティ要件を掲げる組織も存在する。

【００１６】

なお、米国特許第５，８０５，８２０号には、ＤＮＳにおいて、ドメインの内部情報に対する問い合わせ要求をリダイレクト（redirect）することで、組織内ネットワークのドメイン名及びＩＰアドレス等のネットワーク構成情報（private information）をＤＮＳを通じて組織外に送信しないようにした方法及びこれを実現する装置について提案されているが、ＤｏＳアタック等の問題には対処できていない。

【００１７】

したがって本発明は、上記問題点に鑑みてなされたものであって、その目的は、組織外の者が組織のネットワーク構成情報を利用して組織のネットワークに侵入を行う事を防ぐとともに、異常な形式のパケットを受信する事でＤＮＳサーバの動作が異常になる事を未然に防ぐ、ＤＮＳサーバフィルタ及び記録媒体を提供

することにある。

【００１８】

【課題を解決するための手段】

前記目的を達成する本発明のＤＮＳサーバフィルタは、受信したＤＮＳパケットについて、該パケットをＤＮＳサーバに渡すまえに、該パケットに異常があるか否か検査するパケット検証手段を備え、異常を検出した際に、エラー応答パケット生成して、要求元に返す、構成とされている。

【００１９】

本発明は、ＤＮＳプロトコルにおける端末及びＤＮＳサーバからの問い合わせ、及びＤＮＳサーバからの応答パケットを受信するパケット受信部と、問い合わせ要求を管理するためのセション管理テーブルを備え、問い合わせ及び応答パケットを管理し全体の制御を行うセション管理部と、問い合わせ及び応答パケットが異常であるか否かを検査するパケット検証部と、ＤＮＳサーバへの問い合わせパケットを生成する要求生成部と、問い合わせパケットの送信元に返す応答パケットを生成する応答生成部と、問い合わせ及び応答パケットを送信するパケット送信部と、を備え、受信したＤＮＳパケットについて該パケットをＤＮＳサーバに渡すまえに、内容に異常があるか否か検査し、異常を検出した際に、エラー応答パケット生成して要求元に返す。

【００２０】

【発明の実施の形態】

本発明の実施の形態について説明する。本発明のＤＮＳ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｙｓｔｅｍ）サーバフィルタは、ＲＦＣ（Ｒｅｑｕｅｓｔ　Ｆｏｒ　Ｃｏｍｍｅｎｔｓ）１０３４、１０３５、及びこれに関連するＲＦＣ文書により定義されたＤＮＳプロトコルによりＩＰアドレスとホスト名及びドメイン名の対応を関連付けるサービスを行うＤＮＳサーバを含むネットワークシステムにおいて、ＤＮＳパケットを、ＤＮＳサーバに渡す前に、その内容を検査し、異常があれば、エラー応答を返し、検査のための処理を、利用者が追加及び削除する事を可能としている。

【００２１】

本発明によれば、

・外部ネットワークからの異常な形式のＤＮＳパケットを受信することによりＤＮＳサーバが異常動作を引き起こすこと、

・内部ネットワークのホストが異常な形式のＤＮＳパケットをＤＮＳサーバが外部ネットワークに送信することで外部ネットワークに属するホストを異常動作させること、

・組織外の侵入者が内部ネットワークの情報を得るために外部ネットワークからアクセスして内部ネットワークの名前情報を取得すること、等のセキュリティ上の攻撃から、内部ネットワークのＤＮＳサーバと内部ネットワークシステムを防御し、外部ネットワークに対してＤＮＳプロトコルを通じて異常な動作を引き起こさせたり、セキュリティ上の攻撃を行うことを防ぎ、ＤＮＳに関する問題の素早い対応を可能としている。

【００２２】

本発明は、ＤＮＳプロトコルにおける端末及びＤＮＳサーバからの問い合わせ、及びＤＮＳサーバからの応答パケットを受信するパケット受信部（２）と、ＤＮＳ問い合わせ要求を管理するためのセション管理テーブル（８）を備え、問い合わせ及び応答パケットを管理し全体の制御を行うセション管理部（３）と、問い合わせ及び応答パケットが異常であるか否かを検査するパケット検証部（４）と、ＤＮＳサーバへの問い合わせパケットを生成する要求生成部（５）と、問い合わせパケットの送信元に返す応答パケットを生成する応答生成部（６）と、問い合わせ及び応答パケットを送信するパケット送信部（７）と、を備え、受信したＤＮＳパケットについて該パケットをＤＮＳサーバに渡す前に、内容に異常があるか否か検査し、異常を検出した際に、エラー応答パケット生成して要求元へ返す。

【００２３】

パケット検証部（４）が、検証プログラムのエントリポイントアドレスと、検証プログラムの実行の優先順位と、検証プログラムの属性情報とを備えたプログラム管理テーブル（４０）を備え、前記検証ソフトウェアの属性を参照し、実行すべき検証プログラムを選択して実行に移す制御を行う呼出管理部（３０）と、

管理ツールもしくは設定ファイルで指示された検証プログラムの実行ファイルをメモリ上にロードし、ロードされた検証プログラムを初期化し、検証プログラムのエントリポイントを入手した属性と共に前記呼出管理部のプログラム管理テーブルに登録し、及び前記管理ツールで削除を指示された検証プログラムのメモリ上からの解放処理を行うロード管理部（３６）と、検証プログラムから呼び出されるＤＮＳサーバフィルタ本体の機能を利用するためのサブルーチン群よりなるサービスルーチン（３１）と、を備えている。

【００２４】

本発明は、その好ましい一実施の形態において、セション管理テーブル（８）が、要求パケットへのポインタ（６０）と、問い合わせ要求を行った要求元のＩＰアドレス（６１）と、問い合わせ要求を行った要求元ポート番号（６２）と、問い合わせ要求のパケット形式が正常であった場合に問い合わせ要求を別のＤＮＳサーバに転送しているかどうかを示すフラグと（６３）、を備え、パケット受信部（２）がＤＮＳパケットを受信すると、該パケットを前記セション管理部（３）に渡し、セション管理部（３）は、セション管理テーブル（８）に、受信したパケットの送信元のＩＰアドレス、受信したパケットのポート番号を設定し、テスト中を意味する値をフラグを設定したのち、セション管理部（３）は、受信パケットをパケット検証部（４）に渡してパケットの検査を依頼し、パケット検証部（４）でパケットの検査を行い、検査結果に問題がある場合、前記セション管理部（３）が受信パケットの種別を調べ、それが問い合わせ要求であるか否か判定し、問い合わせ要求であれば、前記セション管理部は、前記応答生成部（６）に対して、エラー応答パケットの生成を依頼し、生成されたパケットを前記セション管理テーブル（８）の要求元ＩＰアドレス、ポート番号で指定される相手に対して、パケット送信部（７）に送信を依頼し、受信した応答パケットについて、セション管理テーブル（８）に登録された情報を削除し、受信した問い合わせ要求パケットを解放する。

【００２５】

また受信パケットが問い合わせ要求でない場合、セション管理部（３）が、セション管理テーブル（８）を検索して、元の問い合わせ要求に関する部分を取り

出し、検索されたセション管理テーブル（８）のエントリの要求パケットへのポインタから、問い合わせ要求パケットを参照して、これを基に、応答生成部（６）に対して、エラー応答パケットの生成を依頼し、セション管理テーブル（８）の要求元ＩＰアドレス、及びポート番号で指定される相手に対して、生成した応答パケットを送信するように、パケット送信部（７）に対して依頼し、受信した応答パケットについて、セション管理テーブル（８）に登録されている情報を削除して応答パケットを解放するとともに、該応答パケットに対応する問い合わせ要求について、セション管理テーブルに登録されているエントリも削除する。

【００２６】

またパケット検証部（４）でパケットの検査を行い、検査結果に問題がない場合、セション管理部（３）が受信パケットの種別を調べ、応答パケットの場合、セション管理部（３）は該応答パケットに対応する問い合わせ要求の情報を、前記セション管理テーブル（８）から検索し、セション管理部（３）が受信した応答パケットが元の問い合わせ要求に対する回答となっているかどうかを調べ、調査の結果、さらに問い合わせを行う必要があれば、セション管理部（３）は、受信した応答パケットの情報から次の問い合わせ先を決定し、セション管理部（３）は、要求生成部（５）に問い合わせ要求パケットの生成を依頼し、前記パケット送信部（７）に対して次の問い合わせ先への送信を依頼し、セション管理部（３）は、受信した問い合わせの途中経過である応答パケットに関する情報を前記セション管理テーブルから削除し応答パケットを解放し、前記調査の結果、元々の問い合わせパケットに対する回答となる応答パケットを受信した場合、セション管理部（３）は、応答パケットを受信した応答パケットの結果を反映させた元の問い合わせ要求に対する応答パケットの生成を前記応答生成部（６）に依頼し、パケット送信部（７）に元の問い合わせ要求の送信元に対して送信を依頼し、受信した応答パケットに関連する情報をセション管理テーブル（８）から削除し、元の問い合わせ要求に関する情報を前記セション管理テーブル（８）から削除し応答パケットを解放する。

【００２７】

受信したパケットが問い合わせ要求である場合、セション管理部（３）が受信

パケットの送信元を調べ、前記送信元が組織内部のネットワークからの問い合わせでない場合、組織外のネットワークの問い合わせ要求を解決するために前記セション管理部は、まず最初に問い合わせる組織外のＤＮＳサーバを決定し、元の問い合わせ要求を元にした問い合わせ要求の生成を要求生成部（５）に依頼し、その問い合わせ要求パケットを、前記決定されたＤＮＳサーバに対して送信するようにパケット送信部に対して依頼し、前記送信元が組織内部のネットワークからの問い合わせである場合、セション管理部（３）は受信した問い合わせ要求パケットを元に要求生成部（５）に問い合わせ要求パケットの生成を依頼し、ＤＮＳサーバに対する問い合わせパケットの送信をパケット送信部（７）に依頼し、セション管理部（３）は、受信したパケットに対応するセション管理テーブル（８）のエントリ中のフラグに、「問い合わせ中」の値を設定し、受信パケットへのポインタをセション管理テーブル（８）のエントリのポインタに設定する。

【００２８】

本発明においては、（ａ）ＤＮＳプロトコルにおける端末及びＤＮＳサーバからの問い合わせ、及びＤＮＳサーバからの応答パケットを通信装置を介して受信するパケット受信処理と、

（ｂ）ＤＮＳ問い合わせ要求を管理するためのセション管理テーブルを備え、問い合わせ及び応答パケットを管理し全体の制御を行うセション管理処理と、

（ｃ）問い合わせ及び応答パケットが異常であるか否かを検査するパケット検証処理と、

（ｄ）ＤＮＳサーバへの問い合わせパケットを生成する要求生成処理と、

問い合わせパケットの送信元に返す応答パケットを生成する応答生成処理と、

（ｅ）問い合わせ及び応答パケットを通信装置を介して送信するように制御するパケット送信処理と、

を備え、受信したＤＮＳパケットについて該パケットをＤＮＳサーバに渡すまえに、内容に異常があるか否か検査し、異常を検出した際に、エラー応答パケット生成して返す、ＤＮＳサーバフィルタの前記各処理は、コンピュータ上で実行プログラムを実行することで実現される。この場合、該プログラムを記録した記録媒体からプログラムを読み出し装置を介して、もしくは通信媒体を介してダウ

ンロードしてコンピュータに読み出しインストールし該プログラムの実行形式をコンピュータの主メモリにロードして実行することで、本発明のＤＮＳサーバフィルタを実施することができる。

【００２９】

【実施例】

本発明の実施例について図面を参照して以下に説明する。図１は、本発明の一実施例のＤＮＳサーバフィルタの構成を示す図である。図１を参照すると、ＤＮＳサーバフィルタ１は、ＤＮＳプロトコルにおける端末及びＤＮＳサーバからの問い合わせ及びＤＮＳサーバからの応答パケットを受信するパケット受信部２と、問い合わせ及び応答パケットを管理し全体の制御を行うセション管理部３と、問い合わせ及び応答パケットが異常であるか否かを検査するパケット検証部４と、ＤＮＳサーバへの問い合わせパケットを生成する要求生成部５と、問い合わせパケットの送信元に返す応答パケットを生成する応答生成部６と、問い合わせ及び応答パケットを送信するパケット送信部７と、を備えて構成されている。またセション管理部３は、ＤＮＳ問い合わせ要求を管理するためのセション管理テーブル８を持つ。

【００３０】

図２は、本発明の一実施例のＤＮＳサーバフィルタ１をファイアウォール内に実装した場合の構成の一例を示す図である。図２において、ファイアウォール１０は、インターネットの様な、これが置かれる組織の管理外のネットワーク１５と、組織内のネットワーク１６とを、セキュリティを保ちながら相互接続する役割を持ち、ＤＮＳについて、

・ネットワーク１５に属する端末１７がネットワーク１６に属する端末１８のホスト名とＩＰアドレスの情報やネットワーク１６の名前空間に関する情報を取得すること、

・端末１７からネットワーク１５を通じてＤＮＳサーバ１１に対してＤＮＳプロトコル上不正なパケットを送付することで、ＤＮＳサーバ１１に動作異常を引き起こすこと、

・端末１８やＤＮＳサーバ１１が端末１７やネットワーク１５に属するホスト

に対してＤＮＳプロトコル上異常なパケットを送付すること、

を防ぐ機能を具備することが要請されており、本発明の一実施例においては、ＤＮＳサーバフィルタ１により、これらの機能要件を満たしている。

【００３１】

ＤＮＳサーバ１１は、ＮＩＣ（Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）１３が属するサブネットワーク等のネットワーク１５のＤＮＳ情報の一部と、ネットワーク１６のＤＮＳ情報の一部を管理し、ＤＮＳプロトコルに従い問い合わせに対する応答する機能を持つ。

【００３２】

ＴＣＰ／ＩＰドライバ１２は、ＮＩＣ１３及びＮＩＣ１４を通じて、ＴＣＰ／ＩＰプロトコルで通信を行うための制御を行うものであり、ＤＮＳサーバフィルタ１やＤＮＳサーバ１１はこのＴＣＰ／ＩＰドライバ１２上で動作するプロセスである。

【００３３】

また、ファイアウォール１０は、端末１７から直接ＴＣＰ／ＩＰプロトコルにより端末１８と通信を行うことを許可しない設定（一般的にこの様な設定をＩＰ　ｆｏｒｗａｒｄ（フォワード）がｏｆｆ（オフ）であるという）となっており、ＤＮＳサーバフィルタ１はＮＩＣ１３、ＤＮＳサーバ１１はＮＩＣ１４のＩＰアドレス宛に送付された問い合わせ要求のみ受け付けるように設定されている。

【００３４】

図３は、本発明の一実施例のＤＮＳサーバフィルタ１を１台の装置に実装し、組織のネットワークに設置した場合の構成を示す図である。図３において、ファイアウォール２０は、パケットフィルタリング型ファイアウォールであり、図２のファイアウォールとは異なり、組織外ネットワーク１５に属する端末１７と組織のネットワーク１６に属する端末１８間での直接のＴＣＰ／ＩＰプロトコルによる通信を、ファイアウォール２０の設定により、許可されたポートやアドレスに限り可能としている。

【００３５】

図３において、ファイアウォール２０は、ネットワーク１６を保護する目的で

設置され、ＤＮＳプロトコルについてみると、端末１７がネットワーク１５を経由してＤＮＳプロトコルでアクセスできるのは、ＤＮＳサーバフィルタ１のみであり、組織内のＤＮＳサーバ１１にはアクセスが許可されておらず、また、ＤＮＳサーバ１１や端末１８も、直接ＤＮＳプロトコルでネットワーク１５上のホストへのアクセスは許可されていない設定とされている。

【００３６】

組織のネットワーク１６に属するファイアウォール２０、ＤＮＳサーバフィルタ１、ＤＮＳサーバ１１、端末１８の間は、ＤＮＳプロトコルに限らず、任意のＴＣＰ／ＩＰ上のプロトコルで通信可能である。

【００３７】

ＤＮＳサーバ１１は、ＤＮＳサーバフィルタ１に対してフォワーダの設定を行っている。即ち、ＤＮＳサーバ１１に対して、端末１８からのネットワーク１５に属する端末１７のドメイン名やＩＰアドレスの問い合わせ要求を受信すると、ＤＮＳサーバ１１は、該問い合わせ要求が、ネットワーク１６に属さないホストに関するものであると認識し、該問い合わせ要求を、ＤＮＳサーバフィルタ１に転送（フォワード）する。また端末１８が参照するＤＮＳサーバは、ＤＮＳサーバ１１に設定されている。

【００３８】

図４は、本発明の一実施例のＤＮＳサーバフィルタ１におけるパケット検証部４の構成を示す図である。図４を参照すると、呼出管理部３０は、検証プログラム（ソフトウェア）３２、３３、３４、３５の属性を参照して実行すべきものを選択して実行に移す制御を行うものであり、検証プログラムを管理するためのプログラム管理テーブル４０を備えている。

【００３９】

ロード管理部３６は、

・管理端末を備え操作指示情報を入力する管理ツール３８、もしくは設定ファイル３９の情報で指示された検証プログラムの実行ファイル３７を不図示のメモリ（ＤＮＳサーバフィルタが実装されるコンピュータのメモリ）上にロードする処理、

・メモリ上にロードされた検証プログラムの初期化処理を実行させ、

・検証プログラムのエントリポイントを入手した属性と共に呼出管理部３０が持つプログラム管理テーブル４０に登録する処理、

・管理ツール３８で削除を指示された検証プログラムのメモリ上からの解放処理、

を行う。

【００４０】

サービスルーチン３１は、検証プログラム３２、３３、３４、３５の開発を容易にするための検証プログラムから呼び出されるＤＮＳサーバフィルタ本体の機能を使うためのサブルーチン群である。

【００４１】

図７は、図４のプログラム管理テーブル４０のエントリの一例である。テーブルの各エントリは、

・検証プログラムのエントリポイントアドレス５０と、

・検証プログラムにより指定される実行の優先順位５１と、

・検証プログラムにより指定される検証プログラムの属性５２と、を備えて構成されている。

【００４２】

図８は、本発明の一実施例のＤＮＳサーバフィルタにおけるセション管理テーブル８のエントリの一例である。テーブルの各エントリは、

・要求パケットへのポインタ６０と、

・問い合わせ要求を行った要求元ＩＰアドレス６１と、

・問い合わせ要求を行った要求元ポート番号６２と、

・問い合わせ要求のパケット形式が正常であった場合に問い合わせ要求を別のＤＮＳサーバに転送しているかどうかを示すフラグ６３と、を備えている。

【００４３】

図５及び図６は、ＤＮＳサーバフィルタ１の動作処理を説明するためのフローチャートである。図９は、図４のパケット検証部４の検証プログラムの実行のフローチャートである。

【００４４】

本発明の一実施例のＤＮＳサーバフィルタ１の動作について以下に説明する。

【００４５】

まず、図１、図５乃至図８を参照して、ＤＮＳサーバフィルタ１の動作について説明する。

【００４６】

ステップＳ１０１において、ＤＮＳパケットを、パケット受信部２が受信すると、そのパケットをセション管理部３に渡し、ステップＳ１０２では、セション管理部３は、管理テーブル８にその受信したパケットの送信元のＩＰアドレスを項目６１（図８参照）に、受信したパケットのポート番号を項目６２に入れ、フラグ６３に「テスト中」を意味する値を設定する。

【００４７】

次のステップＳ１０３において、セション管理部３は、受信パケットを、パケット検証部４に渡してパケットの検査を依頼し、パケット検証部４でパケットの検査を行う。

【００４８】

ステップＳ１０４において、パケット検証部４による検査結果に問題があるか否か判定し、正常終了すれば（問題がない場合）、ステップＳ１１１に進み、異常終了すれば、ステップＳ１０５に進む。

【００４９】

ステップＳ１０５では、セション管理部３が受信パケットの種別を調べ、それが問い合わせ要求（ＤＮＳ要求）か否か判定し、ＤＮＳ要求であれば、ステップＳ１０６、応答パケットであればステップＳ１０８に進む。

【００５０】

ステップＳ１０６では、この情報の問い合わせ元に対してエラー応答を返さなければならない状態であるため、セション管理部３は、応答生成部６に対して、エラー応答パケットの生成を依頼し、生成されたパケットを、管理テーブル８の項目６１、６２の相手に対して、パケット送信部７に送信を依頼する。

【００５１】

次のステップＳ１０７では、受信した応答パケットについて、管理テーブル８に登録された情報を削除し、受信した問い合わせ要求パケットを解放して終了する。

【００５２】

一方、ステップＳ１０５において、受信パケットがＤＮＳ要求でなく、ステップＳ１０８に移行するという状態は、以前、このＤＮＳサーバフィルタ１に対して正常な問い合わせ要求が送られ、別のＤＮＳサーバに対して問い合わせ要求を行っている状態であるが、その結果が異常であったため、元々の問い合わせ要求を行ったホストに対して、問い合わせが失敗したことを示すエラー応答を返さなければならないことを意味している。このため、ステップＳ１０８では、セション管理部３が、セション管理テーブル８を検索して、元の問い合わせ要求に関する部分を取り出す。

【００５３】

次のステップＳ１０９では、検索された管理テーブル８のエントリの項目６０から、問い合わせ要求パケットを参照して、これを基に、応答生成部６に対して、エラー応答パケットの生成を依頼し、管理テーブル８の項目６１、６２の相手に対して、生成した応答パケットを送信するように、パケット送信部７に対して依頼する。

【００５４】

次のステップＳ１１０では、受信した応答パケットについて、管理テーブル８に登録されている情報を削除し、応答パケットを解放し、また、これに対応する問い合わせ要求について、管理テーブル８に登録されているエントリも削除して、終了する。

【００５５】

ステップＳ１０４の判定の結果、検査結果正常であった場合には、図６のステップＳ１１１に分岐する。

【００５６】

図６のステップＳ１１１において、セション管理部３が受信パケットの種別を調べ、それが問い合わせ要求パケットであれば、ステップＳ１１９に進み、応答

パケットであればステップＳ１１２に進む。

【００５７】

ステップＳ１１２では、セション管理部３が、この応答パケットに対応する問い合わせ要求の情報を、管理テーブル８から検索する。

【００５８】

次のステップＳ１１３では、セション管理部３が受信した応答パケットが元の問い合わせ要求に対する回答となっているかどうかを調べる。

【００５９】

元々の問い合わせ要求に、ＤＮＳプロトコルにおける再帰問い合わせが指定されていない場合には、そのまま応答パケットとほぼ同じ形の応答パケットを返せば良いが、再帰問い合わせが指定されている場合には、ＤＮＳサーバフィルタ１が回答を得るまでＤＮＳサーバに対して問い合わせを行う必要がある。例えば、“ｗｗｗ．ｆｏｏ．ｃｏ．ｊｐ”というホスト名に対するＩＰアドレスを検索する場合には、

・ルートＤＮＳサーバ、

・“ｊｐ”ドメインを管理しているＤＮＳサーバ、

・“ｃｏ．ｊｐ”ドメインを管理しているＤＮＳサーバ、

・“ｆｏｏ．ｃｏ．ｊｐ”ドメインを管理しているＤＮＳサーバ、

を順に問い合わせることになり、その途中のＤＮＳサーバからは次のＤＮＳサーバのアドレスしか教えてもらえない（例えば“ｃｏ．ｊｐ”ドメインのＤＮＳサーバからは“ｆｏｏ．ｃｏ．ｊｐ”ドメインを管理しているＤＮＳサーバのアドレスについて教えてもらえない）ため、元々の問い合わせ要求に対しては、この応答パケットは問い合わせ途中の状況を示すに過ぎず、回答にはなり得ない。

【００６０】

ステップＳ１１３において、このような調査を行い、さらに問い合わせを行う必要があれば、ステップＳ１１４に、必要がなければステップＳ１１７に進む。

【００６１】

ステップＳ１１４の状態は、ＤＮＳサーバフィルタ１で、さらに他のＤＮＳサーバに対して問い合わせが必要であることを意味している。このため、ステップ

Ｓ１１４において、セション管理部３は、受信した応答パケットの情報から次の問い合わせ先を決定する。

【００６２】

そして、次のステップＳ１１５では、セション管理部３が問い合わせ要求パケットを要求生成部５に問い合わせ要求パケットの生成を依頼し、次の問い合わせ先にパケット送信部７に送信を依頼する。

【００６３】

次のステップＳ１１６では、セション管理部３は、受信した問い合わせの途中経過である応答パケットに関する情報を管理テーブル８から削除し、応答パケットを解放して終了する。

【００６４】

ステップＳ１１７の状態は、元々の問い合わせパケットに対する回答となる応答パケットを受信したことを意味している。このため、ステップＳ１１７では、セション管理部３は、応答パケットを受信した応答パケットの結果を反映させた元の問い合わせ要求に対する応答パケットの生成を応答生成部６に依頼し、パケット送信部７に元の問い合わせ要求の送信元に対して送信を依頼する。

【００６５】

次のステップＳ１１８では、受信した応答パケットに関連する情報を管理テーブル８から削除し、元の問い合わせ要求に関する情報を管理テーブル８から削除し、応答パケットを解放して終了する。

【００６６】

ステップＳ１１１の判定の結果、受信したパケットが問い合わせ要求（ＤＮＳ要求）であれる場合、ステップＳ１１９において、セション管理部３が受信パケットの送信元を調べ、それが組織内部のネットワークからの問い合わせであればステップＳ１２２に進み、そうでなければステップＳ１２０に進む。

【００６７】

ステップＳ１２０の状態は、組織外のネットワークの問い合わせ要求を解決するために、ＤＮＳサーバフィルタ１が問い合わせ元に代わって組織外のＤＮＳサーバに対して問い合わせを開始しなければならないことを意味している。このた

め、ステップＳ１２０では、セション管理部３は、まず最初に問い合わせる組織外のＤＮＳサーバを決定する（多くの場合これは通常ルートサーバである）。

【００６８】

次のステップＳ１２１では、セション管理部３は、元の問い合わせ要求を元にした問い合わせ要求の生成を要求生成部５に依頼し、その問い合わせ要求パケットをステップＳ１２０で決定したＤＮＳサーバに対して送信することをパケット送信部７に依頼する。

【００６９】

一方、ステップＳ１２２の状態は、組織内部のネットワークに関する問い合わせを受けたことを意味する。組織内部のネットワークに関する情報を得るためには、ＤＮＳサーバフィルタ１は、組織内部のＤＮＳサーバ１１に問い合わせを転送（フォワード）する様になっている。

【００７０】

このため、ステップＳ１２２では、セション管理部３は受信した問い合わせ要求パケットを元に要求生成部５に問い合わせ要求パケットの生成を依頼し、ＤＮＳサーバ１１に問い合わせパケットをパケット送信部７に送信を依頼する。

【００７１】

ステップＳ１２３の状態は、問い合わせ要求を受信して現在ＤＮＳサーバフィルタ１が別のＤＮＳサーバに問い合わせを行っていることを意味している。このため、ステップＳ１２３では、セション管理部３は、受信したパケットに対応する管理テーブル８のエントリ中のフラグ６３に、「問い合わせ中」の値を入れ、受信パケットへのポインタを管理テーブル８のエントリ中の項目６０に入れて終了する。

【００７２】

次に、図９を参照して、パケット検証部４について説明する。

【００７３】

ステップＳ２０１では、パケット検証部４の呼出管理部３０が持つ管理テーブル４０を検索して、管理テーブル４０中の優先順位５１が最も大きい値のエントリを探し（実装では、各エントリは優先順位順に並んでいることが望ましい）、

エントリを確定する。

【００７４】

次のステップＳ２０２では、未参照のエントリがあるかどうかを調べ、未参照のエントリが存在する場合、ステップＳ２０３に進む。

【００７５】

ステップ２０３では、呼出管理部３０が、管理テーブル４０のエントリ中の属性５２を調べて、対応する検証プログラムを実行すべきか否かを判断する。

【００７６】

属性５２は、各検証プログラムにより指定され、ＤＮＳサーバフィルタ１の初期化時に、設定ファイル３８により、もしくは、実行中に、管理ツール３８により、ロード管理部３６による検証プログラムファイル３７のロード後の検証プログラムの初期化処理時にロード管理部３６に渡る値をロード管理部３６が設定するものであり、問い合わせ要求パケットのチェックを行うもの、応答パケットのチェックを行うものといった検証プログラムの種類を示す値である。

【００７７】

次のステップＳ２０４では、管理テーブル４０の当該エントリに対応する検証プログラムを呼出管理部３０が実行することに決定した場合、ステップＳ２０５に、そうでない場合はステップＳ２０７に進む。

【００７８】

ステップＳ２０５では、呼出管理部３０は、管理テーブル４０の項目５０にある検証プログラムのエントリポイントを呼び出す。

【００７９】

ステップＳ２０６において、呼出管理部３０は、ステップＳ２０５で呼び出した検証プログラムの結果を見て、正常終了か否か判定し、正常終了した場合ステップＳ２０７に進み、異常終了した場合、検証プログラムでエラーが発生した、すなわち受信したＤＮＳのパケットは組織のセキュリティ要件に合致しない等の理由により受け付けられないと判断されたことになるため、エラーをパケット検証部４の呼出元であるセション管理部３に渡して終了する。

【００８０】

ステップＳ２０７では、次の検証プログラムによる受信パケットのチェックを行うため、呼出管理部３０は、先に行った検証プログラムの次に優先順位が高いもしくは同じ優先順位である検証プログラムを、管理テーブル４０の優先順位５１を参照して検索を行い、ステップＳ２０２に進む。

【００８１】

この様にして、パケット検証部４は、ステップＳ２０２からステップＳ２０７を繰り返し、ステップＳ２０２において、これ以上実行する検証プログラムが存在しないと判断された場合、これまで実行された全ての検証プログラムが正常終了したことを意味しており、受信したＤＮＳパケットは組織のセキュリティ要件を満たしたものであることから、パケット検証部４は正常終了する。

【００８２】

次に、具体例に即して説明する。

【００８３】

図２は、ＤＮＳサーバフィルタ１をファイアウォール１０内に実装した場合の構成を示す図である。組織外のネットワーク１５に属する端末１７が、組織内のネットワーク１６に属する端末１８のＩＰアドレスを取得しようと試みたとする。端末１７は端末１８のホスト名は知っているがその情報が格納されているＤＮＳサーバは知らないものとする。

【００８４】

まず端末１８は、組織外ネットワーク１５に属するＤＮＳサーバから組織のドメインを管理しているＤＮＳサーバの情報を入手し、そのＩＰアドレスがファイアウォール１０のＮＩＣ１３に対応するＩＰアドレスであることが判明する。

【００８５】

次に端末１７は、組織のＤＮＳサーバと思っているファイアウォール１０のＮＩＣ１３のＩＰアドレス上で待ち合わせているＤＮＳサーバフィルタ１に接続し、端末１８のホスト名に対応するＩＰアドレスを問い合わせる。

【００８６】

問い合わせ要求を受けたＤＮＳサーバフィルタ１は、パケット検証部４を呼び出して、このＤＮＳパケットが組織のセキュリティ要件を満たすかどうかを検査

する。

【００８７】

もし、端末１７が送信したＤＮＳパケットの形式が異常であり、検証プログラムとして、これを検査するものが含まれていれば、そのパケットに対して検証プログラムはエラーを返し、ＤＮＳサーバフィルタ１は、端末１７に対してエラー応答を返す。

【００８８】

もし端末１７が送信したＤＮＳパケットの形式が正常であるが、検証プログラムに、組織内部のホストに関する情報は提供しないことをセキュリティ要件を実現するためのプログラムが登録されている場合には、そのパケットに対して、検証プログラムはエラーを返し、ＤＮＳサーバフィルタ１は端末１７に対してエラー応答を返す。

【００８９】

もし端末１７が送信したＤＮＳパケットの形式が正常であるが、検証プログラムに組織内部のホストに関する情報は提供しないことをセキュリティ要件を実現するためのプログラムが登録されていない場合には、ＤＮＳサーバフィルタ１はＤＮＳサーバ１１に要求を転送して端末１８のＩＰアドレスを取得して応答として端末１７に返す。

【００９０】

次に、図２に示した構成において、端末１８が端末１７のＩＰアドレスを入手する場合について説明する。

【００９１】

まず端末１８は、組織内ネットワーク１６のＤＮＳサーバに組織外ネットワークの情報を要求するため、そのＤＮＳサーバはその問い合わせをファイアウォール１０のＮＩＣ１４で待ち合わせているＤＮＳサーバ１１に転送する。

【００９２】

ＤＮＳサーバ１１は、組織外ネットワークについての問い合わせはＤＮＳサーバフィルタ１１に転送する様に設定されている。

【００９３】

問い合わせ要求パケットを受け取ったＤＮＳサーバフィルタ１は、そのＤＮＳパケットが正常であることを確認すると、組織外のＤＮＳサーバに問い合わせ、応答パケットを得て、そのパケットが正常であれば、ＤＮＳサーバ１１を通じて端末１８に結果が返される。

【００９４】

もし端末１７のＤＮＳサーバが異常な応答パケットを返してきた場合には、ＤＮＳサーバフィルタ１はＤＮＳサーバ１１にエラー応答を返し、端末１８にもそのエラー応答が返る。

【００９５】

異常な応答パケットとしては、例えば、形式が異常である他に、組織外との通信を盗聴する等の目的でＤＮＳパケットの付加情報に偽の情報が書き加えられているといった事例が報告されている。

【００９６】

図３は、ＤＮＳサーバフィルタ１が独立して組織内ネットワーク１６に設置された例である。

【００９７】

図３に示す構成において、ＤＮＳパケットのやりとりは、上述した図２に示すものとほぼ同じである。図２に示す構成では、端末１７が直接ＤＮＳサーバ１１にアクセスすることがＴＣＰ／ＩＰドライバ１２で禁じられているのに対し、図３に示す構成では、パケットフィルタ型ファイアウォール２０により、禁止の設定が行われる点が相違している。

【００９８】

本発明においては、パケット検証部４にあらかじめ登録しておいたドメインに属するホストに対する問い合わせがあった場合には、否定応答をを返すように判断する処理を実装することで、ＷＷＷサーバにおける「コンテンツフィルタリング」と呼ばれる技術の様な、組織の業務に無関係なホストへのアクセスを禁止するという要件を満たすためのシステムを構築することができる。

【００９９】

また、本発明においては、ＤＮＳサーバフィルタに、ＤＮＳサーバ情報をあら

かじめ蓄えておくキャッシュメモリを追加することで、余分な問い合わせを減らすことができる。

【０１００】

前記実施例では、本発明を説明するために、セキュリティに関連する処理を例に説明したが、本発明は、セキュリティに関連する目的にのみに限定されるものでないことは勿論である。

【０１０１】

【発明の効果】

以上説明したように、本発明によれば、組織外の者が組織外のネットワークから送信するホスト名、ドメイン名、ＩＰアドレス等の情報をＤＮＳプロトコルを通じて取得するためのＤＮＳパケットを検査し、異常があればエラー応答を返す構成としたことにより、

・組織外の者が組織のネットワーク構成情報を利用して組織のネットワークに侵入を行うこと、及び、

・異常な形式のパケットを受信する事でＤＮＳサーバの動作が異常になること、を未然に防ぐことができる、

という効果を奏する。

【０１０２】

また本発明によれば、組織内の者が組織外のネットワークに属するＤＮＳサーバに送信するホスト名、ドメイン名、ＩＰアドレス等の情報をＤＮＳプロトコルを通じて取得するためのＤＮＳパケットを検査し、異常があればエラー応答を返す構成としたことにより、組織外のネットワークに属するＤＮＳサーバの動作を異常にさせる事未然に防ぐ事が可能となり、組織外のネットワークに属する他組織に対する組織の管理責任を果たすことができる、という効果を奏する。

【０１０３】

本発明のＤＮＳサーバフィルタのパケット検証手段において、利用者による追加及び削除を可能とし、検証プログラムの記述方法を明示して、利用者自身で検証プログラムの作成を可能としたことにより、新たに判明したＤＮＳサーバの問題に利用者による素早い対処を可能とし、またＤＮＳサーバ自体を問題に対応さ

れたものに置換する場合は、問題に対応する不要な検証プログラムを削除してＤＮＳサーバフィルタの性能を向上させることができる、という効果を奏する。

【図面の簡単な説明】

【図１】

本発明の一実施例のＤＮＳサーバフィルタの構成を示す図である。

【図２】

本発明の一実施例のＤＮＳサーバフィルタをファイアウォール内に実装した場合の構成を示す図である。

【図３】

本発明の一実施例のＤＮＳサーバフィルタを１台の装置に実装し、組織のネットワークに設置した場合の構成を示す図である。

【図４】

本発明の一実施例におけるパケット検証部の構成を示す図である。

【図５】

本発明の一実施例におけるＤＮＳサーバフィルタの処理を説明するためのフローチャートである。

【図６】

本発明の一実施例におけるＤＮＳサーバフィルタの処理を説明するためのフローチャートである。

【図７】

本発明の一実施例におけるパケット検証部のプログラム管理テーブルのエントリの一例を示す図である。

【図８】

本発明の一実施例におけるセション管理テーブルのエントリの一例を示す図である。

【図９】

本発明の一実施例におけるパケット検証部の検証プログラムの処理手順を示すフローチャートである。

【符号の説明】

１　ＤＮＳサーバフィルタ

２　パケット受信部

３　セション管理部

４　パケット検証部

５　要求生成部

６　応答生成部

７　パケット送信部

８　管理テーブル（セション管理テーブル）

１０　ファイアウオール

１１　ＤＮＳサーバ

１２　ＴＣＰ／ＩＰドライバ

１３、１４　ＮＩＣ

１５、１６　ネットワーク

１７、１８　端末

２０　ファイアウォール

３０　呼出管理部

３１　サービスルーチン

３２～３５　検証プログラム

３６　ロード管理部

３７　検証プログラム

３８　管理ツール

３９　設定ファイル

４０　管理テーブル（検証プログラム管理テーブル）

５０　エントリポイントアドレス

５１　優先順位

５２　属性

６０　要求パケットへのポインタ

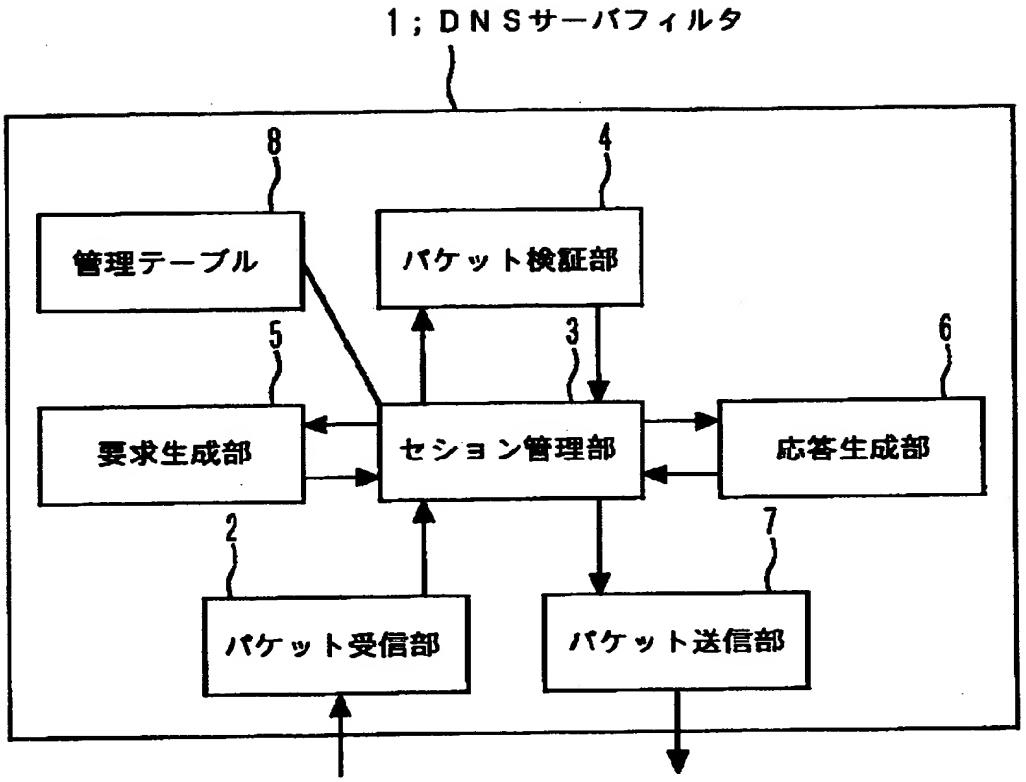
６１　要求元ＩＰアドレス

６２　要求元ポート番号

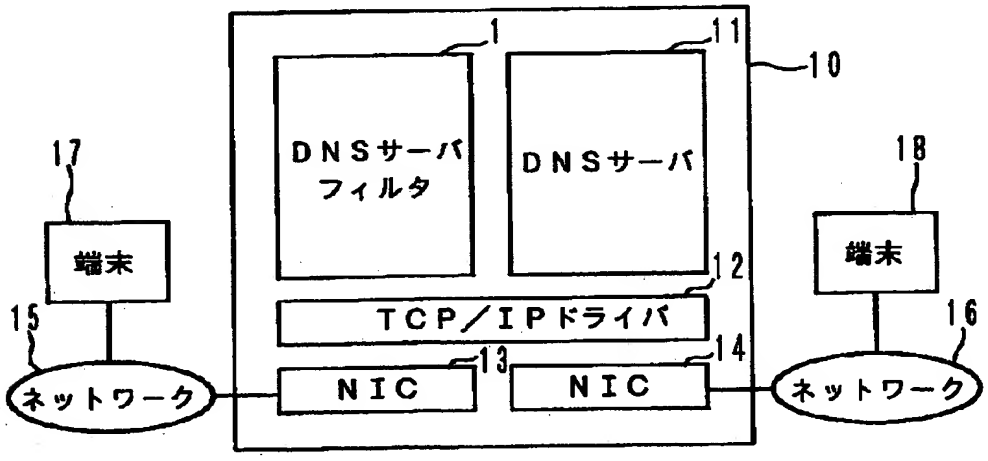
６３　フラグ

【書類名】　　図面

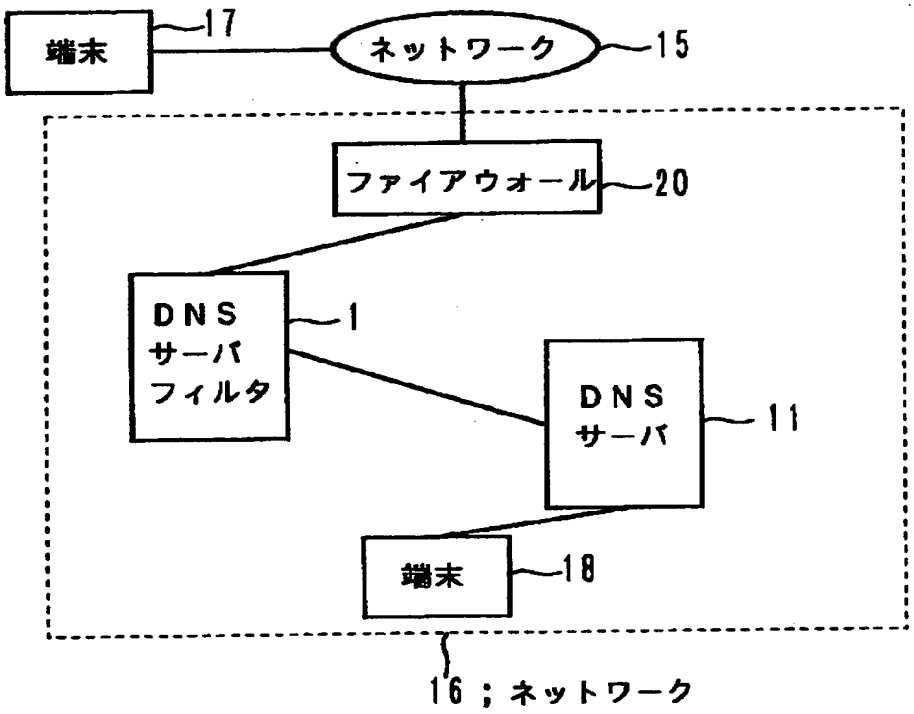
【図１】


1；ＤＮＳサーバフィルタ
8
管理テーブル
4
パケット検証部
5
3
6
要求生成部
セション管理部
応答生成部
2
7
パケット受信部
パケット送信部

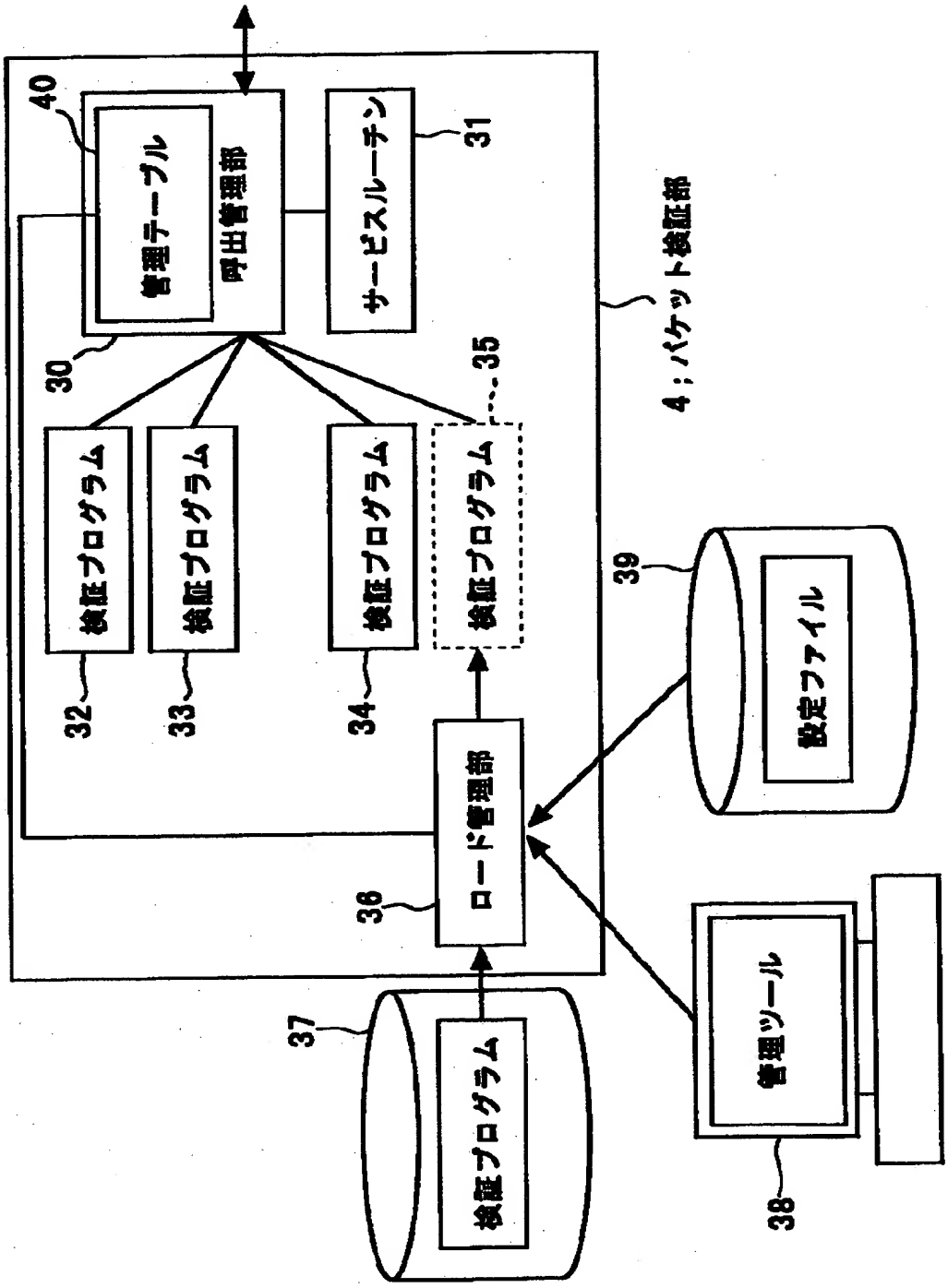
【図２】


1
11
10
ＤＮＳサーバ
フィルタ
ＤＮＳサーバ
17
18
端末
端末
12
ＴＣＰ／ＩＰドライバ
15
16
13
14
ＮＩＣ
ＮＩＣ
ネットワーク
ネットワーク

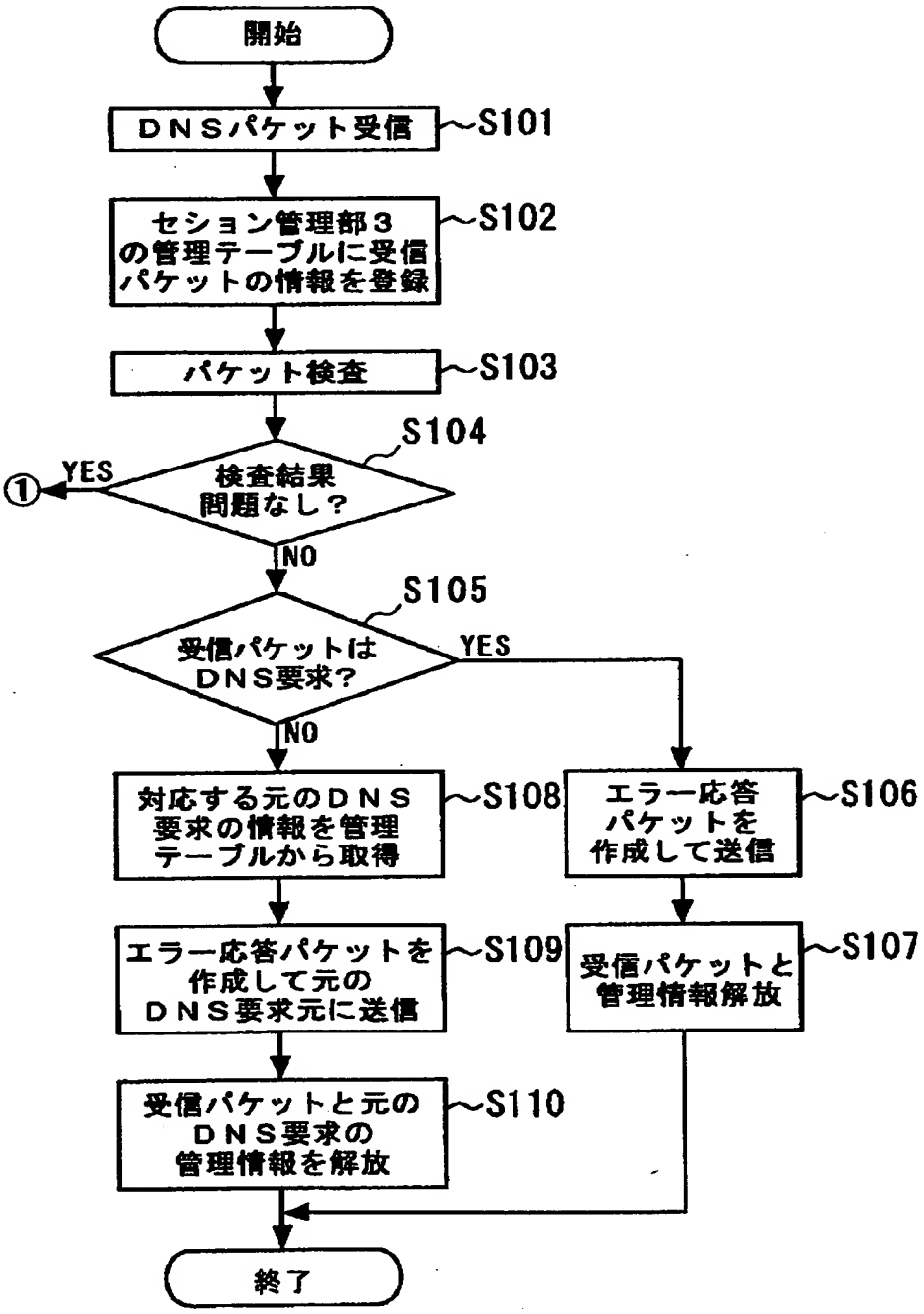
【図３】


端末
17
ネットワーク
15
ファイアウォール
20
DNS
サーバ
フィルタ
1
DNS
サーバ
11
端末
18
16；ネットワーク

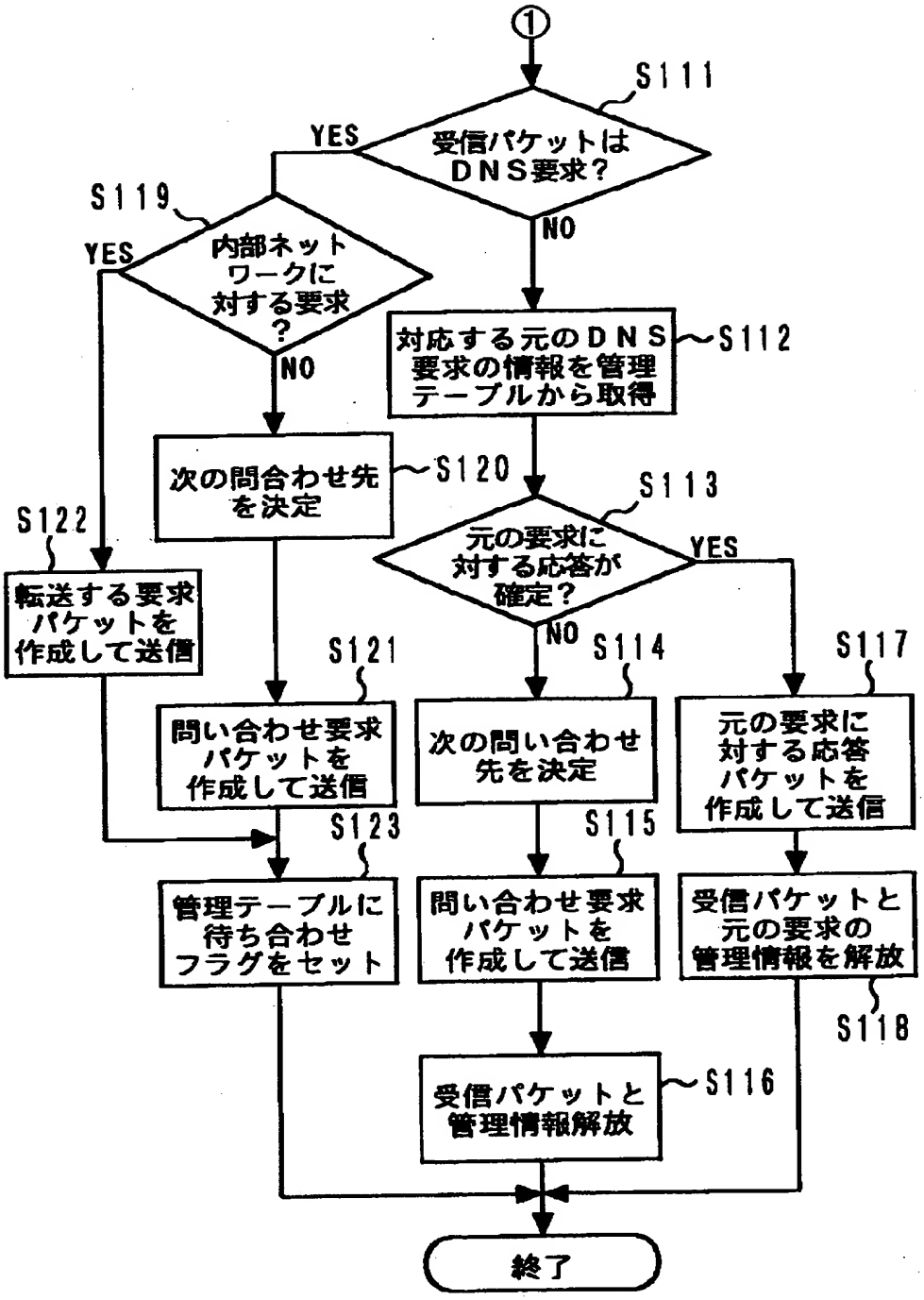
【図４】


4；パケット検証部
40
管理テーブル
呼出管理部
サービスルーチン
31
30
35
検証プログラム
検証プログラム
検証プログラム
検証プログラム
32
33
34
39
設定ファイル
ロード管理部
38
37
検証プログラム
管理ツール
38

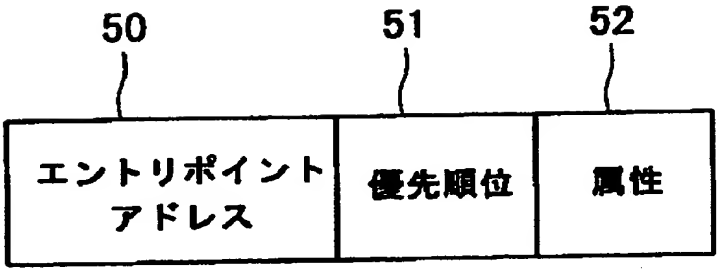
【図５】


開始
DNSパケット受信
S101
セション管理部３の管理テーブルに受信パケットの情報を登録
S102
パケット検査
S103
S104
検査結果問題なし？
YES
①
NO
S105
受信パケットはDNS要求？
YES
NO
対応する元のDNS要求の情報を管理テーブルから取得
S108
エラー応答パケットを作成して送信
S106
エラー応答パケットを作成して元のDNS要求元に送信
S109
受信パケットと管理情報解放
S107
受信パケットと元のDNS要求の管理情報を解放
S110
終了

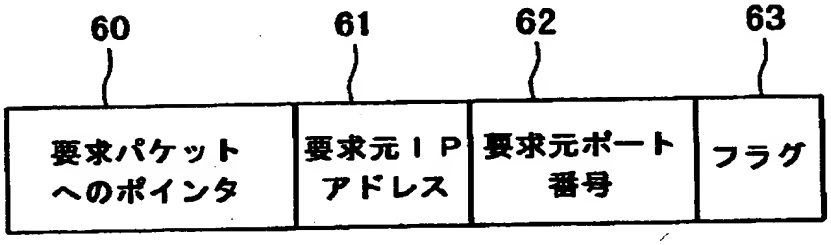
【図６】


①
S111
受信パケットは
ＤＮＳ要求？
YES
NO
S119
内部ネット
ワークに
対する要求
？
YES
NO
対応する元のＤＮＳ
要求の情報を管理
テーブルから取得
S112
次の問合わせ先
を決定
S120
S113
元の要求に
対する応答が
確定？
YES
NO
S122
転送する要求
パケットを
作成して送信
S121
問い合わせ要求
パケットを
作成して送信
S114
次の問い合わせ
先を決定
S117
元の要求に
対する応答
パケットを
作成して送信
S123
管理テーブルに
待ち合わせ
フラグをセット
S115
問い合わせ要求
パケットを
作成して送信
受信パケットと
元の要求の
管理情報を解放
S118
受信パケットと
管理情報解放
S116
終了

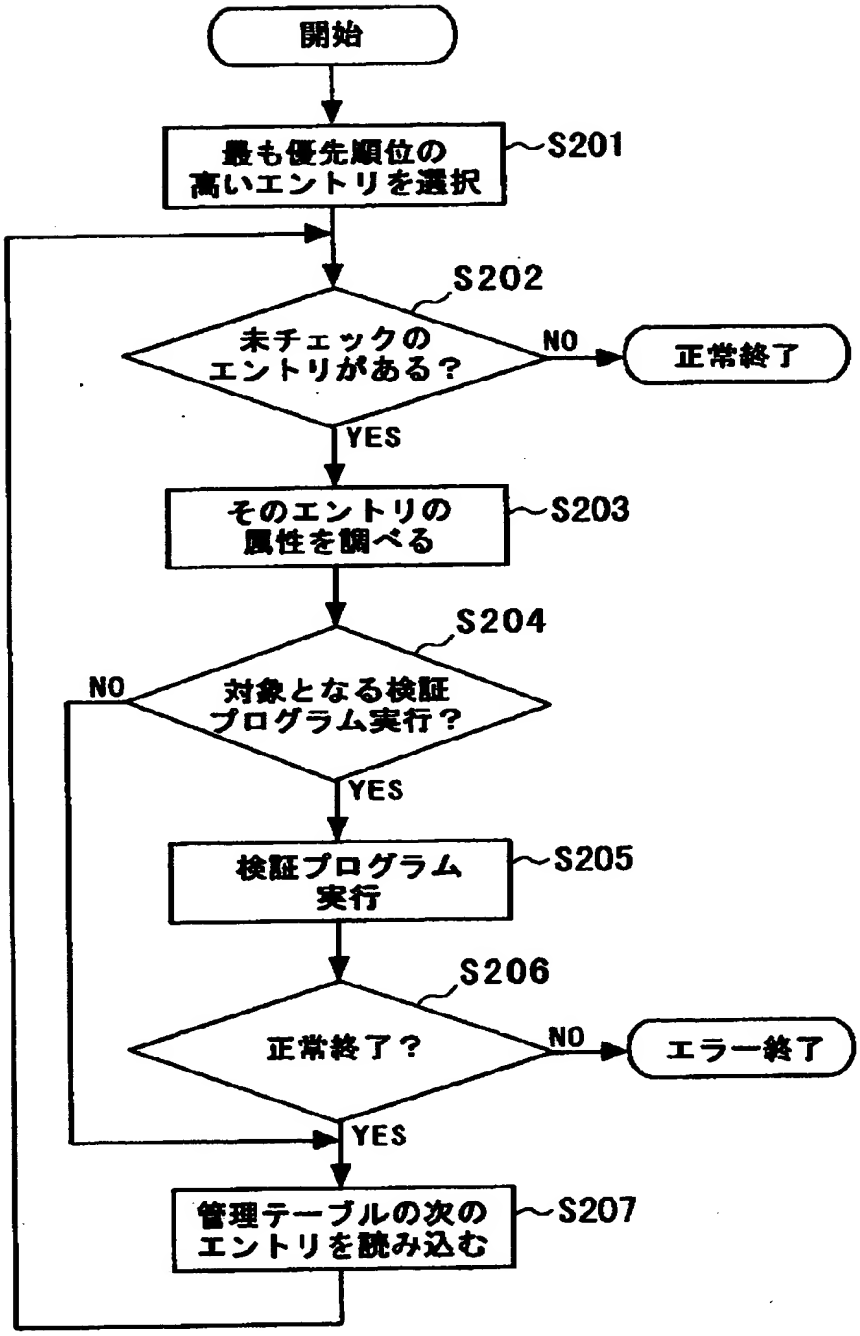
【図７】


50
51
52
エントリポイント
アドレス
優先順位
属性

【図８】


60
61
62
63
要求パケット
へのポインタ
要求元ＩＰ
アドレス
要求元ポート
番号
フラグ

【図９】


開始
最も優先順位の高いエントリを選択
S201
S202
未チェックのエントリがある？
NO
正常終了
YES
そのエントリの属性を調べる
S203
S204
対象となる検証プログラム実行？
NO
YES
検証プログラム実行
S205
S206
正常終了？
NO
エラー終了
YES
管理テーブルの次のエントリを読み込む
S207

【書類名】　　要約書

【要約】

【課題】

組織外の者が組織のネットワーク構成情報を利用して組織のネットワークに侵入を行うことを防ぎ、異常な形式のパケットを受信することでＤＮＳサーバの動作が異常になることを未然に防ぐＤＮＳサーバフィルタの提供。

【解決手段】

ＤＮＳプロトコルにおける端末及びＤＮＳサーバからの問い合わせ、及びＤＮＳサーバからの応答パケットを受信するパケット受信部と、問い合わせ要求を管理するためのセション管理テーブルを備え、問い合わせ及び応答パケットを管理し全体の制御を行うセション管理部と、問い合わせ及び応答パケットが異常であるか否かを検査するパケット検証部と、ＤＮＳサーバへの問い合わせパケットを生成する要求生成部と、問い合わせパケットの送信元に返す応答パケットを生成する応答生成部と、問い合わせ及び応答パケットを送信するパケット送信部と、を備え、受信したＤＮＳパケットをＤＮＳサーバに渡す前に、内容に異常があるか否か検査し、異常を検出した際にエラー応答パケット生成して要求元に返す。

【選択図】

図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
　〔変更理由〕　　新規登録
　　住　所　　東京都港区芝五丁目７番１号
　　氏　名　　日本電気株式会社